FORENSIC MEMORANDUM

CONTACT

TO:	Vipin Shah Spiro Harrison
FROM:	Contact Discovery
SUBJECT:	Server Assessment
DATE:	10/07/2022
CC:	

CONTACT DISCOVERY

Contact Discovery Services, LLC is an independent national ISO:27001 certified digital forensics and electronic discovery firm with offices in Washington D.C., Los Angeles, Boston, New York, and Miami. Contact provides end-to-end litigation support services to the world's top law firms and corporations and has been a trusted partner on a wide range of litigation matters. Contact regularly engages in digital forensic, data processing, analysis, and information management activities supporting large, complex litigations, and internal investigations.

Contact employs a new matter conflict check workflow to eliminate conflicts of interests for all incoming matters. Contact is independent of the Shahs.

ENGAGEMENT & SCOPE

On or about July 20th 2022, Spiro Harrison and Contact Discovery Services, Contact, began discussions surrounding this engagement. Contact was engaged on August 16th, 2022, by Vipin Shah and Spiro Harrison to collect and extract user created content from servers stored at 235 Hillside Avenue, Williston Park, New York 11596.

On August 24th, 2022, Contact retrieved 55 servers from the Hillside facility. This equipment was inventoried onsite and transported to our Washington DC Forensics lab for additional assessments.

On September 30th, 2022, Contact placed the server population into an offsite storage facility.

EVIDENCE SUMMARY

Contact conducted an onsite assessment and retrieval of the servers and associated hardware from the 235 Hillside Avenue location on August 24th, 2022. Jamente Cooper and Josh Blanthorn provided onsite services at the Hillside facility.

Contact collected 55 servers from the Hillside location. These consisted of rack mounted servers varying in sizes with hard drives, internal memory, and internal components structurally complete.

The servers were Dell, HP, and Sun Micro branded products, as well as several custom-built rack mount server systems as well.

235 HILLSIDE AVENUE, WILLISTON PARK, NEW YORK

Contact arrived onsite to the Hillside Avenue location. The defunct facility is configured as a makeshift data center hosted in what was previously a commercial garage, with no climate control or industry-standard protections for the equipment. The location contained servers and racks and associated furnishings to support IT server-based equipment. The equipment contained within was cabled as it might have been when functional, however the servers were not in functional order.

The Hillside location did not have power. The servers were stored without air conditioning, fans, or humidity controls. The facility had pervasive mold extending up the cabling and conduits within the room. The equipment and racks had visible water damage, rust, and mold.

Contact proceeded to remove the equipment from the rack mounts and the cabling. The equipment was then securely packed and transported to our Washington DC digital forensics lab.

Once the assessments were completed all the recovered equipment was moved to an offsite storage location due to the pervasive mold contained within the equipment.

EQUIPMENT ASSESSMENT

Contact accomplished a physical review and assessment across all 55 pieces of hardware retrieved from the Hillside location. This assessment included photographic exhibits of the internal and external components of the servers.

Due to the extensive nature of the environmental damage to physical enclosures, internal electronic hardware, and spinning platter media – i.e. data storage hard drives and the inherent risk associated with powering the equipment on, Contact did not perform a powered assessment of the equipment. The associated water damage creates risk of destruction of data associated with hardware failures within the hard drives.

A. Environmental Damage

Contact noted extensive external environmental damage to equipment stored in the Hillside facility. This included but is not limited to physical degradation of the external cases, connectivity ports and the external screws and bolts holding the server enclosures together as well as the hardware required to rack mount the servers.

B. External Rust

Contact noted physical rust on the outside of the server enclosures, across the top and bottom of the servers, as well as where the server enclosures have rack mounts. We also noted rust that extended into the external connectors of the server enclosures on both the front and rear panels of the servers. We noted internal rust on components and connectors alike.

C. Mold

During our assessment, Contact noted extensive mold across the entire population of equipment. We noted visible mold growing on the internal components of the server equipment. We also noted a strong mold smell coming from the equipment.

DISCOVERY PROCESS

The servers contain some population of user created content along with system files required to operate the computing environment. The goal is maintaining a preservation copy and leveraging that copy to recover reviewable data for the legal team.

In an online server environment, we would create a preservation copy of the target system to ensure a clean, viable, and unaltered copy was created. That preservation copy would be duplicated into a working copy which would be used for downstream work processes.

This requires internal coordination with the team hosting the servers to provide insight into the environment such as which servers host email and files versus a server that hosts databases. This would allow a targeted process rather than imaging all 55 servers.

The coordination would also provide credentials for accessing the servers as well as any encryption keys needed to decrypt the server data.

Once the copy is verified a workflow would be traversed to separate the system files from the user created content, or the reviewable set of data. This data set can be reported upon and then targeted by legal teams for further downstream review.

The servers and environment in this instance are no longer online and appear to have been offline for some time. The process may run into roadblocks around failing equipment, encryption, and the lack of proper credentials to access the servers.

The servers have water damage as indicated by the external rust and pervasive mold. Powering on water damaged equipment creates risk that the internal components fail and crash into the storage platters. This would cause irrecoverable data destruction to the areas where the failure occurs. Both

options A and B have this risk while option C provides a mitigation option for the water damages. It should be noted that there's an additional cost associated with the mitigation efforts ranging between $200,000 - $570,000 prior to the discovery costs associated with extraction and review of user created data.

We can approach the discovery process with one of the workflows described below:

A. Online server discovery

The servers are still structurally complete. We could attempt to power them on and extract live images from the servers despite the inherent risk mentioned above. This would create targeted images of data locations as they would be viewed from the server in a powered and booted state.

We would require administrator usernames and passwords for the servers targeted to access the data. It would be useful to have targeted drives, folders, or locations identified prior to collection. We would need to create a copy of the entire drive without those locations. Review and downstream processing can be targeted with reporting generated from the full images to mitigate reviewing system files or targeted specific locations.

Each server targeted for this process would be connected to a power source, keyboard and mouse, monitor, and encrypted collection media. The target system would then be powered on, and credentials entered. Once active a forensically sound copy process would be completed.

The copy would provide active data without encryption. This data can be directly ingested into standard discovery tools for sampling, analysis, and review.

B. Offline server discovery

The servers while structurally complete, would have the internal drives removed and physically imaged. A forensically sound bit by bit copy would be made of the internal drives. This includes all data stored on the drives including any deleted and potentially recoverable data.

This process does not require upfront usernames and or passwords nor encryption keys. However, they will be required to render the data readable. Encrypted drives will require decryption keys/passphrases to facilitate access to the underlying data.

Servers also leverage RAID technology. This allows multiple physical drives to function as a single storage location, providing additional horsepower and data redundancy. RAID is typically leveraged in server environments, and we would need to rebuild these post-imaging and decryption. This can be a lengthy and time intensive process.

Each server targeted for this process would have the drives inventoried and removed. The drives would then be duplicated. A physical copy of the source drive would be created to a target drive leveraging a physical drive duplicator. The resultant copy can be evaluated for encryption and RAID. Drives without encryption and or RAID can move directly to processing and downstream review. Drives with encryption and or RAID would need further processing as described below.

Once the duplication is completed decryption and RAID rebuilding would ensue. We would require the encryption credentials to decrypt the drives. The decrypted drives would then undergo RAID reconstruction. This process would render an online copy of the data hosted by the target server.

The completed online copy would be duplicated for preservation and downstream processing. This data can then be directly ingested into standard discovery tools for sampling, analysis, and review.

C. Data recovery and discovery

In light of the inherent risk of powering on equipment with water damage, the only option for mitigating this risk would be to send the drives to a specialized outside vendor to work with them. This process would require offline recovery and physical data recovery by the vendor with a clean room and the ability to remove the internal hard drive components from the hard drive enclosures. This mitigates physical damage to the hard drive storage locations that could be incurred by powering on the damaged equipment.

The drives would be removed from the target servers and securely shipped to the clean room lab for recovery. The vendor then undertakes a standard workflow to remove the internal components from the damaged drive enclosures. Those components are then placed into verified working enclosures and physically imaged. The images would then go through one of the recovery methods described above.

CLOSING REMARKS

Beyond the issues mentioned above, it is important to state that imaging and data recovery are where this process begins. Even if we can recover data from the drives while mitigating the water damage and other issues, we still may end up with data we cannot access should we run into issues such as encryption or RAID access to the imaged drives. Additionally, we may run into proprietary systems or software that is no longer available or not supported. Finally, there is the chance that even if all other issues are mitigated and successfully dealt with, the actual data itself may be corrupt and unusable due to the conditions under which it was kept. Each of these steps will incur additional time and costs to address with no guarantee of reviewable data until the very end of the process.

/s/ James O. Whitehead III

James O. Whitehead III

Associate Director of Digital Forensics

10/7/2022

Date

Address:

Contact Discovery Services, LLC

1100 13th St NW Suite 925

Washington, DC 20005